This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

OIPE JC157
JAN 3 0 2004
PATENT & TRADEMARK OFFICE

Attorney's Docket No.: 13913-047001 / 2002P10108 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Karl Goger
Serial No. : 10/722,373
Filed : November 25, 2003
Title : CONTROLLING ACCESS TO ELECTRONIC DOCUMENTS

Art Unit : Unknown
Examiner : Unknown

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF PRIORITY DOCUMENT UNDER 35 USC §119

Applicant hereby confirms his claim of priority under 35 USC §119 from the following application(s):

·European Patent Convention Application No. 02026654.0 filed November 29, 2002

The European Priority Document from which priority is claimed is submitted herewith.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 1/26/04

Spencer C. Patterson
Reg. No. 43,849

Fish & Richardson P.C.
60 South Sixth Street
3300 Dain Rauscher Plaza
Minneapolis, MN 55402
Telephone: (214) 292-4082
Facsimile: (214) 747-2091

90064622.doc

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify under 37 CFR §1.8(a) that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

01/26/2004
Date of Deposit

Signature

Peggy C. Gray
Typed or Printed Name of Person Signing Certificate

Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.	The attached documents are exact copies of the European patent application described on the following page, as originally filed.	Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr.	Patent application No.	Demande de brevet n°
	02026654.0	

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Europäisches Patentamt | European Patent Office | Office européen des brevets

Anmeldung Nr:
Application no.: 02026654.0
Demande no:

Anmeldetag:
Date of filing: 29.11.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

SAP Aktiengesellschaft
Neurottstrasse 16
69190 Walldorf
ALLEMAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method and computer system for protecting electronic documents

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F1/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

METHOD AND COMPUTER SYSTEM FOR PROTECTING ELECTRONIC DOCUMENTS

Field of the Invention

The present invention relates to electronic data processing in general, and particularly to data protection.

Background of the Invention

In organizations, computer systems are used to protect a large amount of electronic documents of various types. The computer systems may be used to perform business processes. Typically, access rights of processes (e.g., business processes) or users often change over time because of

a) the human factor, to change job and responsibility within an organization; or

b) the business factor, that the organization itself changes its processes (e.g., by process reengineering) and/or organizational structure changes; or

c) the business diversification factor, that each organization has different requirements on document access (or document security) with respect to the same type of document depending on organization specific job descriptions and/or specific organizational structures; or

d) the document factor, meaning that new documents are developed which must be easily integrated into an existing computer system without the need to develop a new access control mechanism and/or a user specific document presentation logic for each new type of document.

The following U.S. patents and other references may be useful in respect to document protection.

5,933,498 Schneck et al.
5,991,709 Schoen
6,073,242 Hardy et al.
6,092,090 Payne et al.
6,236,996 Bapat et al.
6,237,099 Kurokawa
6,314,409 Schneck et al

US published applications
20020040370 Entwistle
20020109707 Lao et al.
20020112164 Schmeling et al.

Bapat et al. 6,236,996 shows a data management system that uses an access control database which has access control objects. The access control server provides users access to the managed data objects in accordance with the access rights specified by the access control database. As described in column 9, line 62 et seq. and shown in figures 4-7, the access control tree is comprised of group definitions, user definitions, target definitions, access rules and default rules. Figures 5-7 show actions initiated upon an access request occurring, including processing the request through access rules and confirming or denying the request.

Schneck et al. 5,933,498 shows controlling access and distribution of digital property in accordance with access rights rules. Particular portions of the data may be protected and rules may be determined using different criteria, e.g. user identity, user age. (See also Schneck 6,314,409).

Kurokawa 6,237,099 shows an electronic document management system which determines whether an authorized user has access rights to a particular electronic document using access rights lists.

Hardy et al. 6,073,242 shows an electronic authority server that utilizes multiple roles or a single role (e.g., employee) to ascertain a user's right to access data.

The remaining references are of general interest in regards to document protection. The references show rule based electronic/digital document access rights. These also show determining attributes of an electronic document for various purposes, e.g. content searching, filing based on document type, etc.

Generally speaking these references show access rights in the context of editing (either solo or collaborative editing); accessing a library-type database with little or no focus on editing; or accessing a business-type database of documents such as contracts, medical files, etc.

Some prior art systems use rule based access control, where rules are assigned to the documents or the user directly. When changing the access logic all available documents need to be re-administrated.

Some prior art systems use rules that are implemented in an internal access method, that is, hard coded rules. In such systems, rules are limited to what is coded and, therefore, cannot be dynamically changed or added.

Summary of the Invention

To alleviate the problems of prior art systems the present invention provides computer system, method, and computer program products according to the independent claims.

One aspect of the invention is to provide protection of electronic documents by deriving attributes of electronic documents and incorporating those attributes into rules, in concert with accessor

attributes, for allowing or denying access to the electronic documents.

One embodiment of the present invention provides an authorization system for protecting electronic documents against unauthorized access by using authorization information that is provided by an expert system that operates on top of a knowledge base. The knowledge base includes information, such as, for example, available document types, document structure meta data, document rules, user names, roles (or company job descriptions) or providers of electronic documents.

It is an effect of the present invention that the knowledge base and, therefore, the authorization system can be enhanced/changed by adding or changing rules that use document attributes and accessor attributes without the need to change any application code in the implementation of the presentation logic of the electronic document.

It is a further effect of the invention that the expert system can inspect the documents and document content through a generic interface where the expert system learns about the document and the document structure meta data or other document attributes so that the number of rules is not limited by any number, such as the number of hard coded rules. For example, rules can be based on the document structure meta data and/or any combination of further rules available in the knowledge base.

It is a further effect of the invention that because the access logic is kept separated from the document and user definitions, making a change to the knowledge base affects all documents substantially simultaneously without a need for modifying any document or user definition.

The aspects of the invention will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims. It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention as described.

Brief Description of the Drawings

FIG. 1 is a simplified block diagram of a computer system that can be used with one embodiment of the invention to control access to an electronic document;

FIG. 2A illustrates structure meta data for the electronic document;

FIG. 2B illustrates keys that relate to the structure meta data;

FIG. 3A illustrates how an observer is used to control access to the electronic document while it is edited;

FIG. 3B illustrates how the access behaviour for an accessor in accessing the electronic document can be changed simultaneously for all documents of a specific document type; and

FIG. 4 is a simplified flowchart of a method for controlling access to electronic documents when used with one embodiment of the present invention.

Detailed Description of the Invention

FIG. 1 is a simplified block diagram of a computer system 900 that can be used with one embodiment of the invention to control access to electronic documents. An electronic document is a set of data that is

electronically stored and retrievable. Examples of electronic documents are: a text document, address data of an individual or an organization, an accounting voucher, a production order or any kind of digital data object, e.g., a Word document, an XML document, some Java code, a data object from an object oriented database, and so on. Electronic documents will be referred to as documents in the following description.

The architecture of the computer system 900 defines a closed system, in the sense that an accessor's 200 access to a document (e.g., document 300, 301, 302) or to at least one portion 300-1 of the document is only through a framework 901, and more particularly, through an access layer 902 that is part of the framework 901.

The access layer 902 evaluates authorization information provided by an expert system 904 on request 420. For example, the authorization information includes an access behaviour of the document and/or information about the structure of the document (e.g., document portions, nested documents). As determined by the authorization information, the access layer 902 allows or disallows the accessor to access 460 the document 300 or portion 300-1. The access behaviour can be different for different accessors.

According to the type of the accessor (e.g., user, process, application), the accessor can have attributes 200-A, such as user role, user group, process type or application type. For example, the accessor attribute(s) may be stored in data structures used for user role definitions as available in the R/3 system or in the mySAP Enterprise Portal of SAP AG. In case a user uses an application to access a document, the accessor can be considered as a two-dimensional combination of the user and the application and, therefore, the accessor attributes can also be combinations of multiple one-dimensional accessor

attributes. For example, a two-dimensional accessor attribute can be a combination of a corresponding user role attribute and the corresponding application type. This is true for any multi-dimensional accessor accordingly.

The documents are stored in a repository 903. For example, a document is stored in a central cache. In the framework 901, each type of document can implement a generic interface (in the Java sense of 'interface', a collection of method definitions, declared constants, or both) that the access layer 902 can use to learn characteristics of the document, such as, for example document attributes. Generic interface refers to an interface that is common to all documents of the framework. The generic interface enables the framework to access fields, attributes or portions and paragraphs of a document and to retrieve the corresponding values. In another implementation the invention can also be used with dumb documents in combination with a repository of metadata that provides attributes of the dumb documents. In another implementation the invention can also be used with self describing documents, such as XML documents or JAR files or PDF files, in combination with an external metadata repository and external methods for providing attribute information for the framework.

In the example, document 300 has a document attribute 300-A. Examples of document attributes are document type, document structure information, document meta data, document relationship information or document access behaviour.

What a particular accessor 200 can see and do with respect to a particular document 300 or a portion 300-1 of the document is determined by an expert system 904 based on accessor attributes 200-A, document attributes 300-A, and rules of a rule set 800. If the document has no structure, the portion 300-1 and the document 300

can be considered to be identical. In other words, the expert system 904 determines an access behaviour with regards to the document 300 or portion 300-1 by evaluating rules of a rule set 800 when the accessor 200 tries to access the document 300 or one of its portions (e.g., portion 300-1) by using 410 the access layer 902. The rules reference at least to the document attribute 300-A and the accessor attribute. Examples of access behaviours applicable to any type of document and document granularity (e.g., whole document, portion, child document) are:

a) hidden (the document is hidden),

b) protected (the reader gets an information that there is a document, but can not access the content),

c) read (it is possible to view the document but not to change the content),

d) modify (it is possible to make changes to the content),

e) delete (it is possible to delete the document),

f) create (it is possible to create a document of a specific type), and

g) print (it is possible to print the document)

Further access behaviours can be defined, such as, for example:

j) copy (can create a copy of the document)

k) transport (transport the document to a different data processing system)

l) archive (the document can be sent to a archive)

m) others, where the access logic can be enhanced by using information from the expert system. For example, custom access behaviours can be defined as methods of the corresponding documents. For example, documents can be classes, e.g., Java classes, and the invention can be used to control access to and use of classes (program components).

When the accessor 200 modifies a document, the expert system 904 can track each modification with respect to access violations. In case of an access violation the expert system optionally can inform the accessor by, for example, sending a message, such as "Please change vacation dates during regular working hours only", or "You are not responsible for the selected customer" if the accessor is a human user.

While an accessor is modifying a document the access layer can retrieve allowed document attribute values or combinations of such values from the expert system depending on the document type, the rules and the already existing content of the document. In other words, by calculating allowed values for which the accessor has authorization the expert system provides information that the access layer can use to guide the accessor when modifying a document. For example, a human resource management clerk in an organization is entitled to process employee data for all employees where the last name starts with letters in the range from "G" to "M". In this case, when the clerk uses a possible-entries help function for an input field of a corresponding human resource application, the system will only provide the names of employees starting with a letter within the value range that can be processed by the clerk according to his/her authorization. The present invention enables the access layer to provide values to a user interface layer in accordance with an access behaviour by using the expert system and the knowledge base.

Once the access behaviour is determined, the expert system 904 returns 450 the access behaviour to the access layer 902, which will control the access of the accessor accordingly. A knowledge base 905 can include the definitions of the access behaviours.

Further, the rule set 800 can be implemented in the knowledge base 905. The rules can come from

providers or owners of the documents in the system. For example, the rule set 800 includes rules that use the accessor attribute 200-A and the document attribute 300-A to assert that certain conditions, when true, lead to certain conclusions. The truth of the conditions is determined on the basis of the accessor and document attribute values. The result of the rule evaluation is a proposition about the access behaviour of the accessor relative to the document or to a portion of the document.

Further, the knowledge base 905 can include information about users, information about documents, and meta data information about document structures and document types. The user information can include role attributes for particular users. The document structure information, for example, can include information that a text document can have styles public and private, and a rule of the rule set 800 can define different access behaviours (e.g., permissions to read) to users with different roles.

For example, the expert system 904 checks document attributes, such as, the document type, document structure or document content, depending on information specified in the knowledge base 905 by accessing 430 meta data of the corresponding document type through a further generic interface. Then, the expert system 904 retrieves 440 the corresponding information (e.g., user information, document types, document meta data, document relations, access behaviour definitions or rules) from the knowledge base 905 for determining the access behaviour.

For example, the document structure information can allow the document 300 to include document portions or nested documents, and the permission rules can allow access to an inner portion 300-1 or nested document while disallowing access to an outer portion or the enclosing document.

It is an effect of the present invention that, since all access occurs through the access layer 902, it is possible to change the presentation of the document 300 (e.g., on a display or printout) depending on the authorization information from the expert system in conjunction with the access layer. For example, when a sales clerk calls a sales turnover report document, the clerk may only be authorized to see the monthly turnover of his/her own customers. However, when the clerk's manager calls the same report document, he/she may see a document including multiple portions for various employees of the sales department.

The knowledge base 905, expert system 904, repository 903 and the framework 901 can all be implemented in one computer system as shown in FIG. 1 but can also be implemented in various computer systems that can communicate, for example, over a network.

FIG. 2A illustrates structure meta data 801 for the document 300.

For example, in a first embodiment the document 300 includes two sub-portions 300-2, 300-3. The sub-portion 300-2 is an outer portion 300-2 that further includes the inner portion 300-1. In a second embodiment, the sub-portions are replaced by nested (child) documents that are included by reference. For convenience of explanation the following description is based on the first embodiment but is also true for the second embodiment or any mix of the first and second embodiments.

Structure meta data 801 reflects the structure of document 300. For this example, the structure meta data is stored in the knowledge base 905. Dashed double arrows indicate which portion of the structure meta data 801 corresponds to which portion of the document 300. Document 300 can have a document type that is

assigned to the corresponding structure element D1 in the structure meta data 801. The structure element OP-1 corresponds to the outer portion 300-2. The structure element IP-1, IP-2 correspond to the inner portions 300-1, 300-3, respectively.

A specific access behaviour can be applied to a document as a whole or to portions of the document. The same is true for a nested (child) document of the document and portions of the child document. Each portion/child document can have an access behaviour that is different from that of the document including the portion/child document. The access behaviour of a portion/child document can assign more rights to an accessor than does the access behaviour of the (outer parent) document that includes the portion/child document. In the example of FIG. 2 the access behaviour for the structure element D1 is 'READ ONLY'. However, the access behaviour for the outer portion structure element OP-1 is 'NO ACCESS', whereas the access behaviour for the inner portion structure element IP-1 (and the inner portion IP-2 structure element) is 'MODIFY'. In other words, the access to the inner portion can be controlled so that the document can be accessed by a reader, for example, in a 'read only' mode, whereas the access to the outer portion is prohibited but the inner portion 300-1 of the outer portion 300-2 can be accessed in a 'change' or 'modify' mode. With respect to the inner portion 300-3 document 300 itself can be considered as the outer portion.

FIG. 2B illustrates keys that relate to the structure meta data 801.

A key can be associated (dashed double arrows) with a structure element in the structure meta data 801. For example, structure elements D1, IP-2 and OP-1

are associated with keys 501, 502 and 503, respectively.

The key bit of each key can be considered as a part of the access behaviour for the associated structure element. A key can have a sub-key defining a more restrictive access behaviour than the key itself. For example, a key can allow access to all zip codes complying with the mask "6****", whereas a first sub-key of the key allows access to all zip codes complying with the mask "69***" and a second sub-key allows access to all zip codes complying with the mask "67***". The first sub-key can have a further sub-key that allows access to all zip codes complying with the mask "695**" only, and so on.

Instead of using fixed values for defining a key, the key can also be generically defined by using parameters whose values are automatically determined by the expert system at runtime.

In case a child structure element IP-2 corresponds to a portion of its parent D1, the child structure element can have its own key 502 or inherit the key 501 of its parent D1. In case the child structure element corresponds to another (child) document that is included in the structure meta data by reference, the included (child) document has its own key associated.

It is an effect of the present invention that by associating a key with a structure element of the structure meta data 801, any access behaviour granularity can be achieved with regards to the document, portion or child-document corresponding to the structure element.

FIG. 3A illustrates how an observer is used to control access to a document while it is edited.

As explained in reference to FIG. 1, the access layer 902 allows the accessor 200 to access 460 either a portion 301 or the whole document 300. For example,

rule R1 is used by the expert system to determine the appropriate access behaviour. In case the access behaviour allows the accessor to modify the document 300 or any portion of the document, an observer 701 can track events that are raised 470 by the document 300 or by a runtime representation of the document that is specific to the accessor. This runtime representation will be referred to as container. When an accessor gets access to the document, the framework 901 generates a corresponding container that references the document, so that, for example, the accessor can modify the document through the container. The container reflects the access behaviour of the accessor with respect to the document. That is, although the container knows the full structure of the document, it restricts the accessor's view on the document in accordance with the access behaviour. Because the container knows the full structure of the document it can detect an access violation, whenever the accessor tries to access portions of the document that are not permitted or when the accessor tries to perform an action that does not comply with the access behaviour.

In a multi-accessor environment the document 300 can be simultaneously accessed by multiple accessors with various access behaviours through corresponding containers all referencing the same document. The document can be stored in a central cache.

For example, the observer 701 of the document 300 can be implemented as a runtime component of the expert system 904 or of the framework 901. In one embodiment, each document has a corresponding observer. In another embodiment one observer can be used, for example, for multiple documents (e.g., documents having the same document type). The observer 701 receives an event directly from the document 300 or from a corresponding container without going through the access layer 902. When the observer 701 receives the event because, for

example, the content of the document has been modified, the expert system 904 can track the modification (e.g., by using a corresponding document attribute 300-A) and use a different rule R' from the rule set 800 to determine an appropriate access behaviour that can be different from the access behaviour that was applied prior to the modification. For example, an access behaviour "READ ONLY" can be determined and immediately be applied by the access layer to the current accessor 200 with respect to the document 300/portion 300-1 and the corresponding container. In case of multiple accessors working through further corresponding containers on the same document 300, the observer 701 of the document notifies any of the further corresponding containers about the changes so that the change becomes effective for any accessor that processes the document at that moment.

For example, the document can be a purchase order stored in a central cache of an enterprise resource planning (ERP) system. The purchase order can include multiple purchase items (e.g., document portion 300-1). The document attribute 300-A can be a document status that indicates whether or not the purchase order includes open purchase items. Further, the purchase order can have a method that changes the document status 300-A from "open" to "closed" as soon as all purchase items are "closed". An accessor who modifies the document by closing the last open purchase item of the document triggers the corresponding modification of the document status 300-A from "open" to "closed". The document raises 470 a corresponding event that is received by the corresponding observer 701. The observer 701 causes the expert system to retrieve an appropriate updated access behaviour by using a rule (e.g., rule R1') that incorporates the corresponding document attribute value "closed" (instead of the previous value "open" that relates to a different rule,

such as rule R1). For example, the appropriate updated access behaviour can be "READ ONLY". When providing the "READ ONLY" access behaviour to the access layer 902, the access layer immediately takes away from the accessor all permissions that allow the accessor to further modify the content of the document or of any document portion. The remaining permissions only allow the accessor to view the content of the document. That is, the accessor, although not having left the session for editing the document, suddenly is not in a position to apply further modifications to the document.

FIG. 3B illustrates how the access behaviour for an accessor in accessing a document 301 of a specific document type can be changed simultaneously for all documents 301, 302 of the specific document type.

A change of the rule set 800 can affect substantially simultaneously the access behaviour of the accessor 200 relative to the document or to any document portion without the need to change the document or the accessor 200.

For example, the access layer 902 grants 460 the accessor 200 access to the document 301 having a document attribute 301-A. The corresponding access behaviour is determined at the time point T1 by the expert system 904 by using the rule R2 in the rule set 800. For example, at T1, rule R2 includes the information that an accessor 200 with an accessor attribute 200-A having a value, such as "sales organization 1", can modify any document having a document attribute 301-A with a value, such as "customer master data", only if the zip code of a customer's address in the document 301 starts with "6" (6*). In case the responsibility of the sales organization 1 is changed, the corresponding rule R2 can be adjusted accordingly. For example, at T2, rule R2 is adjusted to reflect that sales organization 1 now

is responsible for all customers having a zip code starting with "6" or "7" (6* OR 7*). From T2 onwards any combination of accessor attributes and document attributes that leads to using rule R2 for the determination of the access behaviour results in providing permissions for zip codes 6* OR 7* in the access layer.

FIG. 4 is a simplified flowchart of a method 400 for controlling access to electronic documents. The method 400 includes the steps receiving access request 410, requesting authorization information 420, receiving authorization information 450 and granting access 460.

In the receiving step 410, an access layer 902 receives a request of an accessor 200 to access at least one portion 300-1 of a document 300 stored in a repository 903. The document has at least one document attribute 300-A. The accessor 200 has at least one accessor attribute 200-A. If the document has no structure, the at least one portion corresponds to the document itself. The access layer uses a generic interface of the document to learn about the at least one document attribute.

In the requesting step 420 the access layer requests authorization information from an expert system 904 with regards to the authorization of the accessor 200 to the at least one portion. The access layer provides the at least one document attribute and the at least one accessor attribute to the expert system. The expert system uses the attribute information for retrieving the authorization information including an access behaviour from a knowledge base 904. For this, the expert system applies rules of a rule set 800 to data that includes at least the document attribute(s) and the accessor attribute(s). Besides a data driven (forward) chaining

approach, a goal driven (backward) chaining approach or a mixed approach can also be used with the invention by those skilled in the art. In the forward chaining approach, the expert system first gathers all data (e.g., document and accessor attributes) before starting to evaluate the corresponding rules to determine the access behaviour. In the backward chaining approach the expert system starts with the goal (e.g., a need to change the access behaviour from "READ ONLY" to "MODIFY") and evaluates with gathering the corresponding data when needed. A mixed approach can be advantageous, when forward chaining is done with all the readily available data, and if the accessor hits an access violation (e.g., when trying to perform an activity that is not allowed by the current access behaviour), backward chaining is done to determine whether the access might be permissible after all

For example, the rule set 800 can also be stored in the knowledge base. Rules of the rule set can use the accessor attribute(s) and the document attribute(s). The expert system can also retrieve document meta data from the knowledge base. For example, in case of a document with an internal structure meta data 801 that describes the structure of the document 300 can be retrieved. For each portion of the document, the expert system can determine a specific access behaviour, such as hidden, protected, read, modify, delete, create, print, copy, transport, archive or optional custom access behaviours.

In the receiving authorization information step 450, the access layer receives from the expert system 904 the authorization information including the access behaviour with regards to the at least one portion 300-1 for the accessor 200.

In the granting access step 460, the access layer 902 grants the accessor 200 access to the at least one portion 300-1 according to the access behaviour. For example, if the structure meta data 801 indicates that the at least one portion is an inner sub-portion 300-1 of an outer portion 300-2 of the document 300, the access layer 902 can allow the accessor 200 to access the inner sub-portion 300-1 but prevent the accessor 200 from accessing the outer portion 300-2. The outer portion may also correspond to the whole document 300.

In case changes are applied to the rule set, these changes substantially simultaneously affect the access behaviour to the at least one portion 300-1 without the need to change the document 300 or the accessor 200. Further, any other access behaviour, whose determination by the expert system depends on the change, is affected immediately after the change has occurred. That is, any access to any document by any accessor is evaluated by an access control mechanism according to the present invention that uses the changed rule set immediately after the change has occurred.

When the accessor tries to access the document 300 or the portion 300-1, the framework 901 generates a runtime representation of the document 300 that references the document 300 and reflects the access behaviour with respect to the accessor 200.

The document or the representation (container) may raise an event that is triggered by a change of the document 300. An observer 701 receives the event from the document 300 or the container and causes the expert system 904 to determine an updated access behaviour in accordance with the change. Then, the observer notifies the document 300 and the container about the updated access behaviour. In a multi-accessor case each

container that is connected to the document 300 gets notified.

An embodiment of the present invention can be implemented by using a computer system that has at least a memory and a processor. The computer system can communicate with further computer systems over a network (e.g., a wide area network (WAN), a local area network (LAN), the Internet.) A computer program product that can be loaded into the memory of the computer system includes instructions that when executed by the processor causes the computer system to perform steps according to the present invention.

The invention can be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The invention can be implemented as a computer program product, i.e., a computer program tangibly embodied in an information carrier, e.g., in a machine-readable storage device or in a propagated signal, for execution by, or to control the operation of, data processing apparatus, e.g., a programmable processor, a computer, or multiple computers. A computer program can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one site or distributed across multiple sites and interconnected by a communication network.

Method steps of the invention can be performed by one or more programmable processors executing a computer program to perform functions of the invention

by operating on input data and generating output. Method steps can also be performed by, and apparatus of the invention can be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit).

Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. Information carriers suitable for embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in special purpose logic circuitry.

To provide for interaction with a user, the invention can be implemented on a computer having a display device, e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse or a trackball, by which the user can provide input to the computer. Other kinds of

devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input.

The invention can be implemented in a computing system that includes a back-end component, e.g., as a data server, or that includes a middleware component, e.g., an application server, or that includes a front-end component, e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the invention, or any combination of such back-end, middleware, or front-end components. The components of the system can be interconnected by any form or medium of digital data communication, e.g., a communication network. Examples of communication networks include a local area network ("LAN") and a wide area network ("WAN"), e.g., the Internet.

The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

The invention has been described in terms of particular embodiments. Other embodiments are within the scope of the following claims. For example, the steps of the invention can be performed in a different order and still achieve desirable results.

Claims

1. A computer system (900) for protecting electronic documents comprising:

a repository (903) for storing an electronic document (300) having a document attribute (300-A);

an access layer (902) used (410) by an accessor (200) to access (460) at least one portion (300-1) of the electronic document (300), the accessor (200) having an accessor attribute (200-A); and

an expert system (904) operable to determine an access behaviour with regards to the at least one portion (300-1) by evaluating rules of a rule set (800) with reference at least to the document attribute (300-A) and the accessor attribute when the accessor (200) tries to access the at least one portion (300-1) using (410) the access layer (902).

2. The computer system (900) of claim 1, where the access behaviour is defined in a knowledge base (905).

3. The computer system (900) of claim 2, where the rule set (800) is stored in the knowledge base (905).

4. The computer system (900) of any one of the claims 1 to 3, where the expert system (904) returns (450) the access behaviour to the access layer (902) to control the access of the accessor.

5. The computer system (900) of any one of the claims 1 to 4, where the rule set (800) has a rule that uses the accessor attribute (200-A) and the document attribute (300-A) to assert a condition on the basis of a value of the accessor attribute (200-A) and a value of the document attribute (300-A).

6. The computer system (900) of any one of the claims 1 to 5, where the access layer (902) learns about the document attribute (300-A) of the document (300) by using a generic interface.

7. The computer system (900) of claim 6, where the expert system (904) retrieves structure meta data (801) of the document that describes the structure of the document (300).

8. The computer system (900) of claim 7, where the structure meta data (801) indicates that the at least one portion is an inner sub-portion (300-1) of an outer portion (300-2) of the document (300) and the access layer allows the accessor to access the inner sub-portion (300-1) but prevents the accessor from accessing the outer portion (300-2).

9. The computer system (900) of claim 7, where the structure meta data (801) has at least one structure element (IP-2) that is associated with a key (502) that influences the access behaviour for the at least one structure element (IP-2).

10. The computer system (900) of any one of the claims 1 to 9, where a framework (901) generates a runtime representation of the document (300) that references the document (300) and reflects the access behaviour with respect to the accessor (200).

11. The computer system (900) of any one of the claims 1 to 10, where the document attribute (300-A) is selected from the group of document type, document structure information, document meta data, document relationship information, document access behaviour.

12. The computer system (900) of any one of the claims 1 to 11, where the accessor attribute (200-A) is selected from the group of user role, user group, process type, application type and any combination thereof.

13. The computer system (900) of any one of the claims 1 to 12, where the access behaviour is selected from the group of hidden, protected, read, modify, delete, create, print, copy, transport, archive and custom access behaviour.

14. The computer system (900) of any one of the claims 1 to 13, where the accessor (200) is selected from the group of user, application, process and any combination thereof.

15. The computer system (900) of any one of the claims 1 to 14, where a change of the rule set (800) affects substantially simultaneously the access behaviour to the at least one portion (300-1) without the need to change the document (300) or the accessor (200).

16. A method (400) for controlling access to electronic documents comprising the steps:

an access layer (902) receiving (410) a request of an accessor (200) to access at least one portion (300-1) of an electronic document (300) stored in a repository (903); the electronic document (300) having a document attribute (300-A); the accessor (200) having an accessor attribute (200-A);

the access layer (902) requesting (420) authorization information from an expert system (904) with regards to the authorization of the accessor (200) to the at least one portion (300-1);

the access layer (902) receiving (450) from the expert system (904) the authorization information including an access behaviour with regards to the at least one portion (300-1), where the access behaviour is determined by applying rules of a rule set (800) to data comprising at least the document attribute (300-A) and the accessor attribute (200-A); and

the access layer (902) granting (460) the accessor (200) access to the at least one portion (300-1) according to the access behaviour.

17. The method (400) of claim 16, where the access behaviour is defined in a knowledge base (905) and the rule set (800) is stored in the knowledge base (905).

18. The method (400) of any one of the claims 16 to 17, where the rule set (800) has a rule that uses the accessor attribute (200-A) and the document attribute (300-A) to assert a condition on the basis of a value of the accessor attribute (200-A) and a value of the document attribute (300-A).

19. The method (400) of any one of the claims 15 to 18, comprising the further step:

a framework (901) generating a runtime representation of the document (300) that references the document (300) and reflects the access behaviour with respect to the accessor (200).

20. The method (400) of claim 19, comprising the further steps:

an observer (701) receiving an event from the document (300) or the runtime representation, where the event is triggered by a change of the document (300);

the observer (701) causing the expert system (904) to determine an updated access behaviour in accordance with the change; and

the observer (701) notifying the document (300) and the runtime representation about the updated access behaviour.

21. The method (400) of any one of the claims 15 to 20, comprising the further step:

the expert system (904) retrieving structure meta data (801) of the document that describes the structure of the document (300).

22. The method (400) of claim 21, where the structure meta data (801) indicates that the at least one portion is an inner sub-portion (300-1) of an outer portion (300-2) of the document (300) and the granting step (460) comprises the further steps:
the access layer (902) allowing the accessor (200) to access the inner sub-portion (300-1); and
preventing the accessor (200) from accessing the outer portion (300-2).

23. The method (400) of any one of the claims 15 to 22, where the access behaviour is selected from the group of hidden, protected, read, modify, delete, create, print, copy, transport, archive and custom access behaviour.

24. The computer system (900) of any one of the claims 15 to 23, comprising the further step:
changing the rule set (800); and
affecting substantially simultaneously the access behaviour to the at least one portion (300-1) without the need to change the document (300) or the accessor (200).

25. A computer program product comprising instructions that when loaded into a memory of a computer system (900) causes at least one processor of the computer system (900) to perform steps according to any one of claims 15 to 24.

METHOD AND COMPUTER SYSTEM FOR PROTECTING ELECTRONIC DOCUMENTS

Abstract of the Invention

Computer system (900) and method for protecting electronic documents. The computer system (900) includes a repository (903) for storing an electronic document (300) that has a document attribute (300-A). An access layer (902) is used (410) by an accessor (200) to access (460) at least one portion (300-1) of the electronic document (300). The accessor (200) has an accessor attribute (200-A). An expert system (904) is operable to determine an access behaviour with regards to the at least one portion (300-1) by evaluating rules of a rule set (800) with reference at least to the document attribute (300-A) and the accessor attribute when the accessor (200) tries to access the at least one portion (300-1) using (410) the access layer (902).

FIG. 1

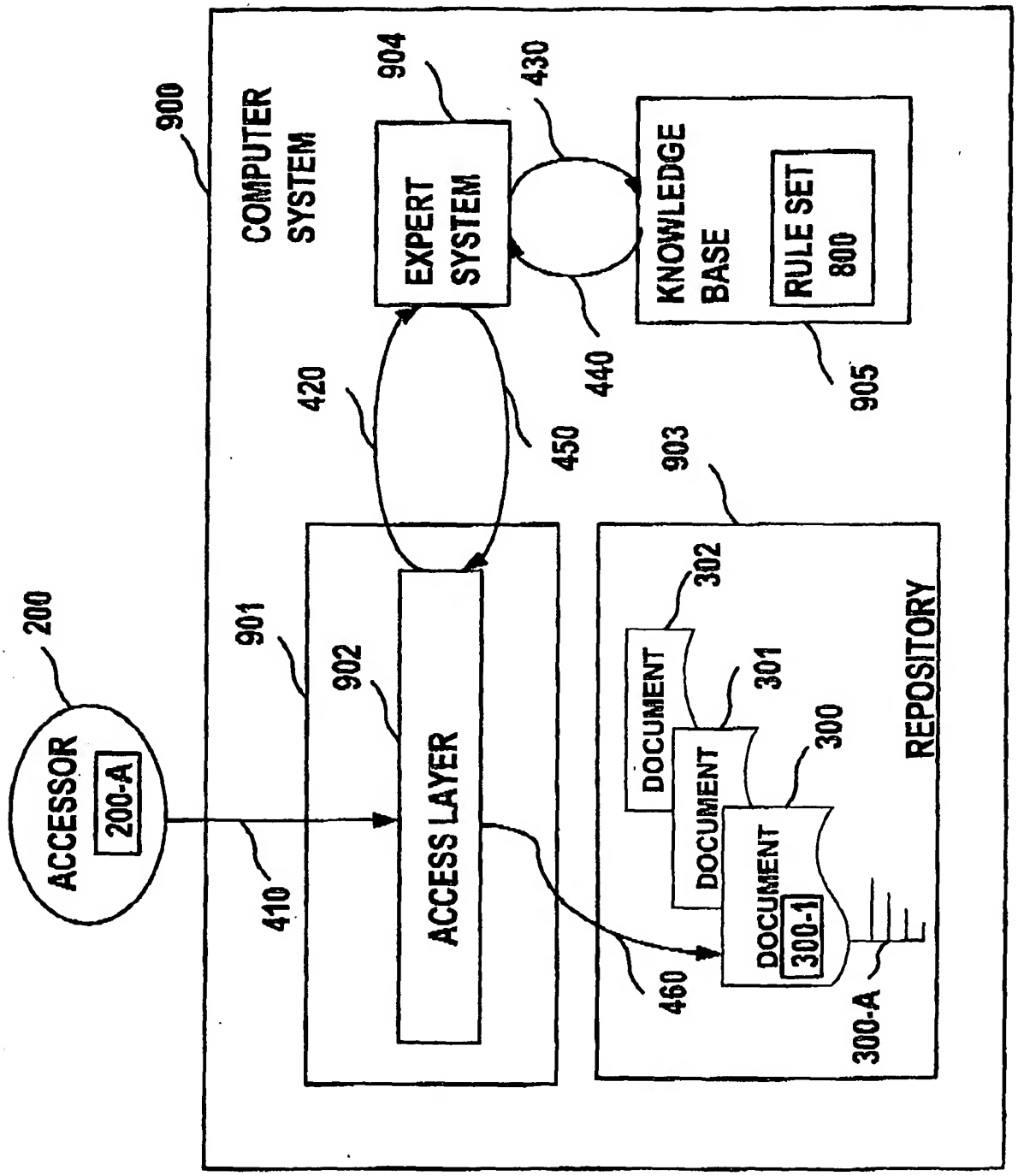
900
COMPUTER SYSTEM
904
EXPERT SYSTEM
430
KNOWLEDGE BASE
RULE SET 800
905
440
420
450
903
200
ACCESSOR
200-A
901
902
ACCESS LAYER
410
460
302
DOCUMENT
301
DOCUMENT
300
DOCUMENT
300-1
REPOSITORY
300-A

FIG. 1

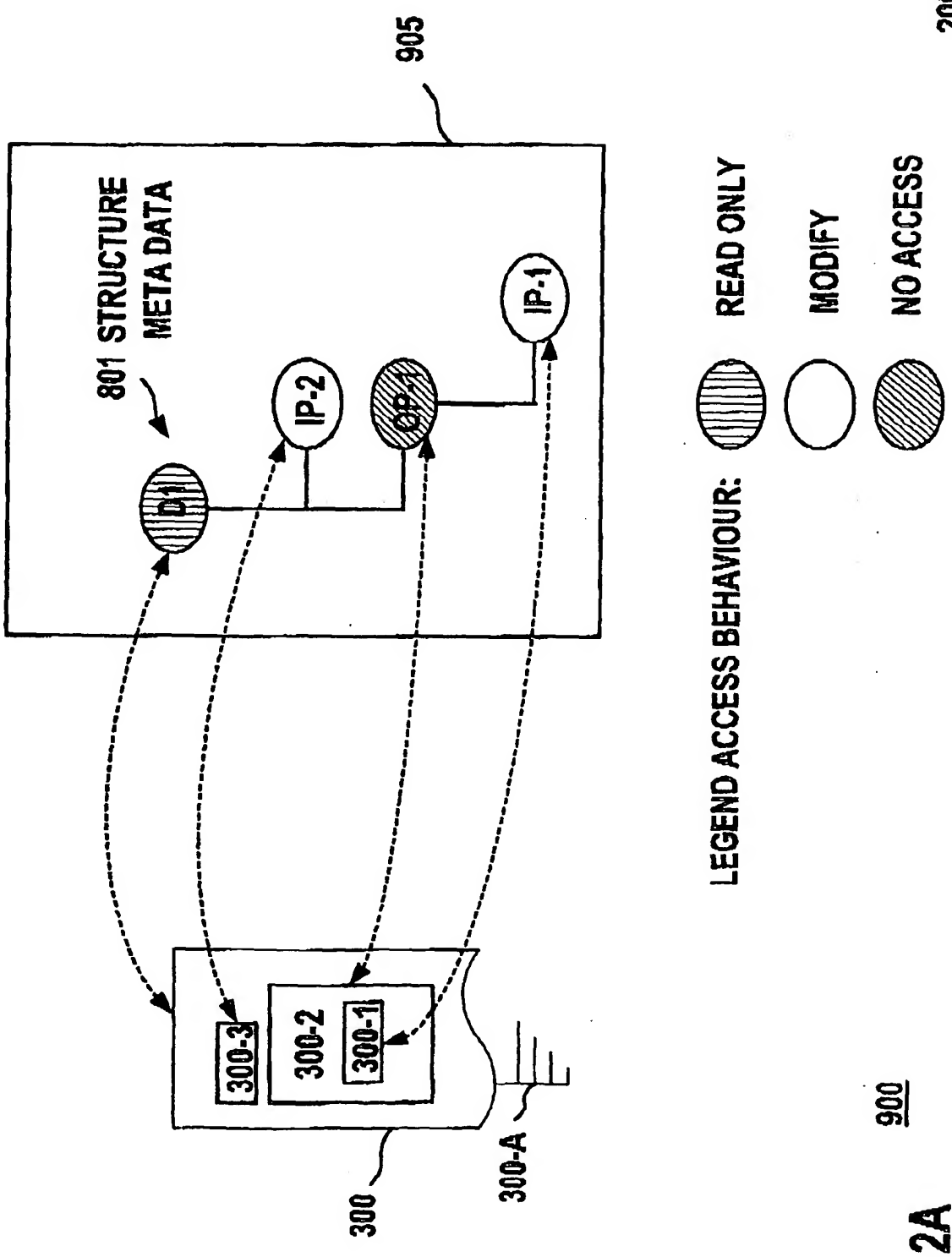
905
801 STRUCTURE META DATA
D1
IP-2
OP-1
IP-1
300-3
300-2
300-1
300
300-A
LEGEND ACCESS BEHAVIOUR:
READ ONLY
MODIFY
NO ACCESS
900

FIG. 2A

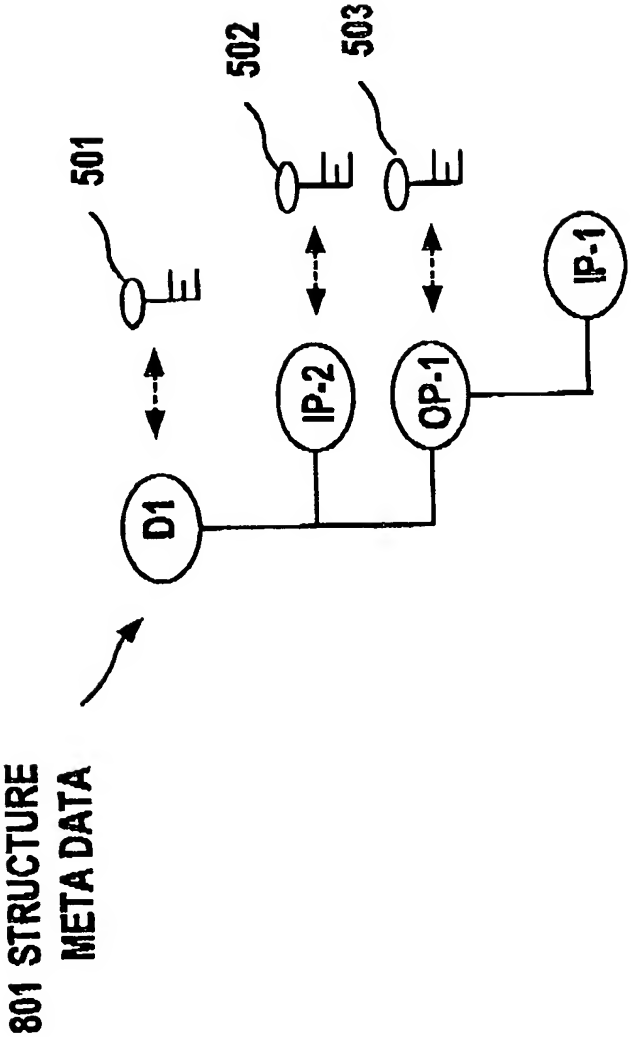

FIG. 2B

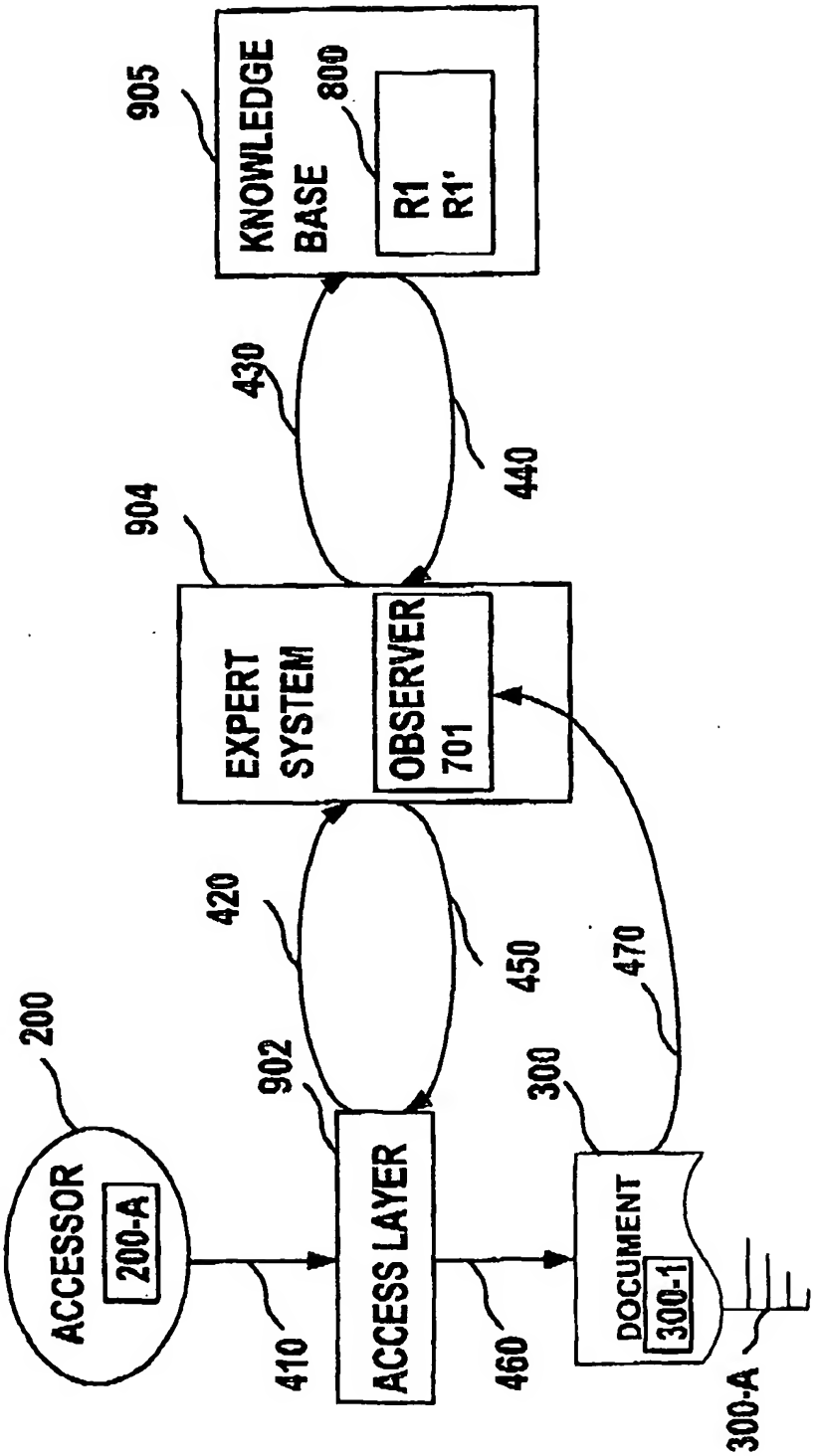
905
KNOWLEDGE BASE
800
R1
R1'
430
440
904
EXPERT SYSTEM
OBSERVER 701
420
450
470
200
902
300
ACCESSOR
200-A
ACCESS LAYER
DOCUMENT
300-1
410
460
300-A

FIG. 3A 900

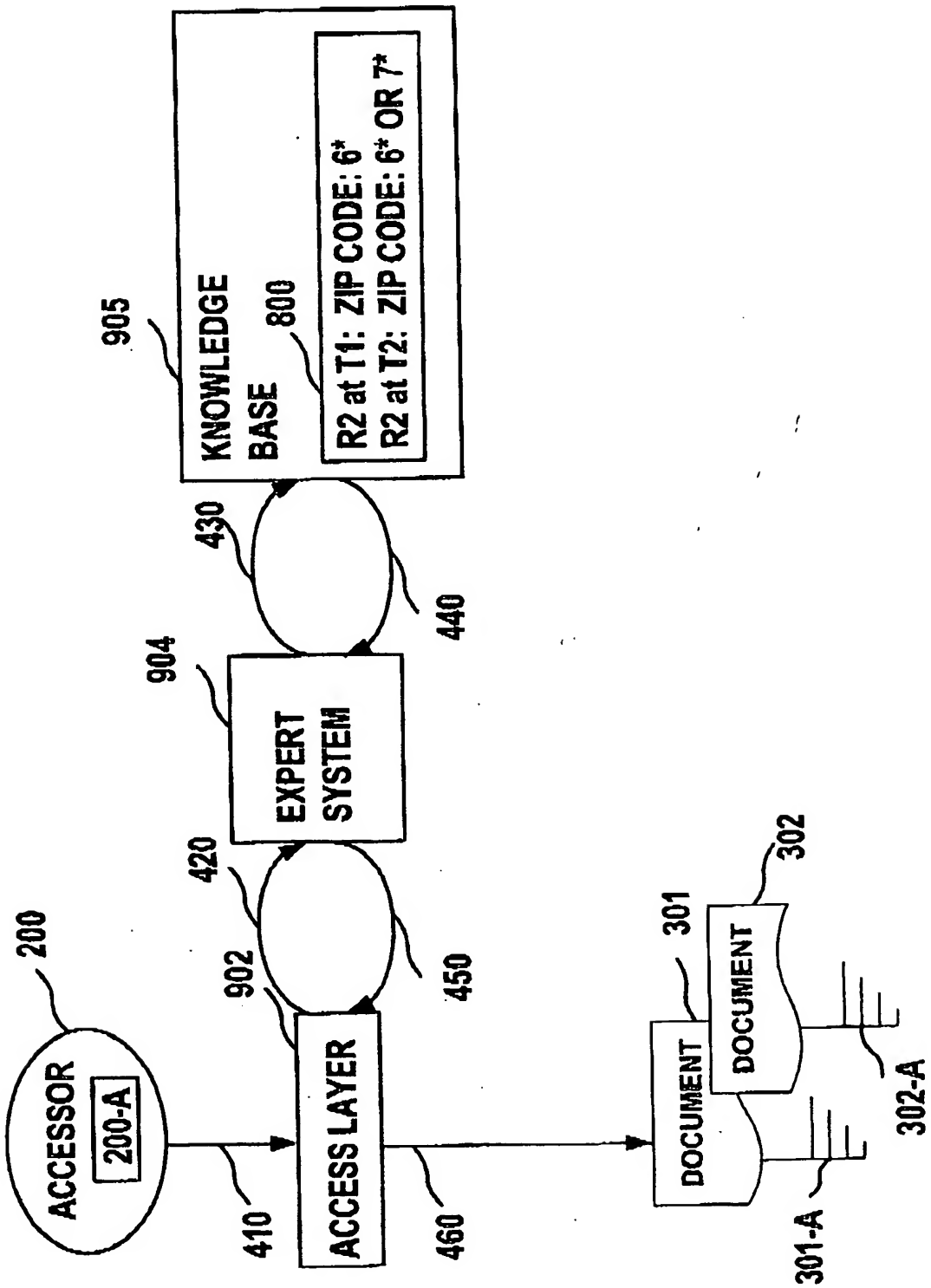
905
KNOWLEDGE BASE
800
R2 at T1: ZIP CODE: 6*
R2 at T2: ZIP CODE: 6* OR 7*
430
440
904
EXPERT SYSTEM
420
450
902
200
ACCESSOR
200-A
410
ACCESS LAYER
460
301
DOCUMENT
302
DOCUMENT
302-A
301-A
900

FIG. 3B

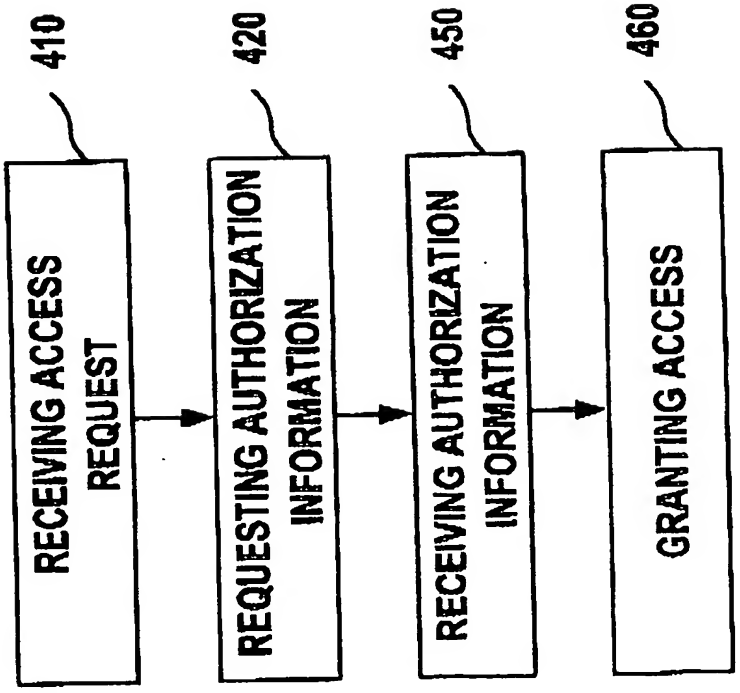
410
RECEIVING ACCESS REQUEST
420
REQUESTING AUTHORIZATION INFORMATION
450
RECEIVING AUTHORIZATION INFORMATION
460
GRANTING ACCESS

FIG. 4 400